UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

GOOD TECHNOLOGY CORPORATION and GOOD TECHNOLOGY SOFTWARE, INC.,

Plaintiffs,

v.

MOBILEIRON, INC.,

Defendant.

Case No. 5:12-cv-05826-PSG

ORDER GRANTING-IN-PART MOTION FOR SUMMARY JUDGMENT OF GOOD TECHNOLOGY'S PATENTS

(Re: Docket No. 218)

Mobile hardware devices rarely secure or manage themselves to anyone's satisfaction. And so those that depend on such devices often turn to specialized security and management software to finish the job. This is a case between companies that supply such software and own patents on the same.

Plaintiffs Good Technology Corporation and Good Technology Software, Inc. own United States Patent Nos. 6,151,606, 7,702,322, 7,970,386 and 8,012,219. On that, Good and Defendant MobileIron, Inc. agree. But they do not agree on much more. Three years ago, Good filed this suit against MobileIron for infringement of its patents. MobileIron not only disputed that it infringes any Good patent, it filed counterclaims that Good infringes its own patent, United States Patent No. 8,359,016. A difficult period of discovery followed.[1]

[1] *See, e.g.*, Docket No. 173; Docket No. 174; Docket No. 229; Docket No. 286; Docket No. 342; Docket No. 343; Docket No. 346.

MobileIron now moves for summary judgment of non-infringement (either literally, by equivalents, willfully or indirectly) of all four asserted Good patents. MobileIron also moves for summary judgment that the '606 patent is invalid for lack of written description. No reasonable jury could find that MobileIron infringes the '606 patent, or that the '606 patent is valid. Nor could that same jury find that MobileIron willfully or indirectly infringed. Because genuine issues of material fact persist, however, as to the remaining patents and theories, the motion is GRANTED but only IN-PART.

I.

The Patent Act requires the patent specification to conclude with "one or more claims particularly pointing out and distinctly claiming the subject matter which the inventor or a joint inventor regards as the invention."[2] While claim construction is a question of law for the court,[3] infringement and validity—in most instances—are questions of fact are reserved for the jury unless no genuine issues remain in dispute.

Good develops and sells mobile data and device management technologies.[4] Good owns United States Patent Nos. 6,151,606, 7,702,322, 7,970,386 and 8,012,219.[5] The '606 patent teaches disabling access to data on a mobile device after the user has finished using the data.[6] The '219 patent teaches a server system that can be used to prevent access to data stored on a mobile device through encryption or deletion.[7] The '386 patent teaches a rules engine on a wireless device that can receive a set of rules from a server and execute the set of rules so as to monitor and take action on the wireless device based on policies.[8] The '322 patent teaches distribution of software

[2] 35 U.S.C. § 112(b).

[3] *See Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 835, 835 (2015).

[4] *See* Docket No. 32 at ¶ 2.

[5] *See id.* at ¶¶ 18-21.

[6] *See* Docket Nos. 32-1, 32-2.

[7] *See* Docket No. 32-5.

[8] *See* Docket No. 32-4.

updates for wireless devices that are governed by customer-defined software policies and communicated over the internet.[9] Good's products include Good for Enterprise, Good for Government, Good Dynamics, BoxTone and AppCentral.[10]

MobileIron is an enterprise mobility management solutions provider, which enables companies to secure, control and manage mobile devices, mobile apps and mobile content.[11] MobileIron owns United States Patent No. 8,359,016, which teaches filtering a catalog of mobile device applications based on a set of policies applied to a user profile and a mobile device profile to select a set of applications to return to the user.[12] MobileIron offers two EMM solutions: MobileIron Core and MobileIron Cloud. MobileIron Core comprises three primary components: the Core server, the Sentry server and the Mobile@Work client. The Core server enables IT administrators to define security policies and to take actions upon mobile devices, apps and content. Sentry is a gateway server that manages and secures network traffic between the mobile devices and corporate systems, such as email and document repository servers. The Mobile@Work client is installed on the mobile device, enforces the security policies received from the Core server and also sends device information back to the Core server.

MobileIron Cloud is MobileIron's cloud-based EMM solution and also has three main software components. The MobileIron Cloud server is the central location from which security policies and actions are defined and implemented. MobileIron Cloud also includes a Sentry gateway server that manages network traffic between the mobile devices and corporate systems. MobileIron Go, the client software, is installed on the mobile device, enforces security policies received from the MobileIron Cloud server and also sends device information back to the

[9] *See* Docket No. 32-3.

[10] AppCentral is a product that allows companies to distribute mobile applications to their users. *See* Docket No. 191-10.

[11] *See* Docket No. 41 at 10.

[12] *See* Docket No. 41-1.

MobileIron Cloud server. MobileIron also offers other various products and features such as Docs@Work, Apps@Work, AppConnect and Email+.[13]

In late 2012, Good sued MobileIron alleging both infringement of the '606, '322, '386 and '219 patents and violations of the Lanham Act and California Business and Professions Code Section 17200.[14] MobileIron counterclaimed, alleging that Good's AppCentral product infringes MobileIron's '016 patent.[15]

II.

This court has subject matter jurisdiction pursuant to 15 U.S.C. § 1125 and 28 U.S.C. §1367. The parties further consented to the jurisdiction of the undersigned magistrate judge pursuant to 28 U.S.C. §636(c) and Fed. R. Civ. P. 72(a).

Pursuant to Fed. R. Civ. P. 56(a), summary judgment is appropriate when "there is no genuine issue as to any material fact and the moving party is entitled to judgment as a matter of law." Material facts are those that may affect the outcome of the case.[16] A dispute as to a material fact is genuine if there is sufficient evidence for a reasonable jury to return a verdict for the non-moving party.[17] All evidence must be viewed in the light most favorable to the non-moving party. At this stage, a court "does not assess credibility or weigh the evidence, but simply determines whether there is a genuine factual issue for trial."[18] Initially, the moving party bears the

---

[13] *See* Docket No. 219-5 at 3.

[14] *See* Docket No. 32.

[15] *See* Docket No. 41.

[16] *See Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 248 (1986) ("Only disputes over facts that may affect the outcome of the suit under governing law will properly preclude the entry of summary judgment. Factual disputes that are irrelevant or unnecessary will not be counted.").

[17] *See id.*

[18] *House v. Bell*, 547 U.S. 518, 559-60 (2006).

burden to show that no genuine issue of material fact exists.[19] If this burden is met, the burden shifts to the non-moving party.[20]

III.

A fundamental issue underlying MobileIron's various challenges to Good's claims is exactly what an ordinarily skilled artisan would understand Good's inventions to be. To be sure, the court has already construed many disputed terms.[21] But the pending motion reveals further construction is required. When that construction is completed, only the '606 patent, as well as Good's willful and indirect infringement theories, may be disposed of as a matter of law. The others require a jury to weigh in.

First, no reasonable jury could find that MobileIron infringed the '606 patent. The '606 patent claims a way for users to access information in a protected manner from an "untrusted client site." To mitigate the risk of subsequent access to that corporate information by an unprivileged user of that same "untrusted client site," a workspace data manager creates a temporary trusted environment in which a user can access corporate information.[22] Upon logout by the user, the "system and method [] advantageously delete downloaded data and all interfaces from the local client, so that no traces are left on the local client for unprivileged users to review."[23] The deletion process happens after the user has finished accessing "the data in a trusted manner at the untrusted client site."[24] The idea is to protect sites where multiple individuals have access on a regular basis.[25]

---

[19] *See Celotex Corp. v. Caltrett*, 477 U.S. 317, 323-24 (1986).

[20] *See T.W. Elec. Serv., Inc. v. Pac. Elec. Contractors Ass'n*, 809 F.2d 630, 630 (9th Cir. 1987).

[21] *See* Docket No. 135.

[22] Docket Nos. 218-5, 218-6, Exh. 7 at 2:9-11.

[23] *Id.* at 3:6-9.

[24] *Id.* at Claims 1, 10, 21.

[25] *See* Docket No. 219-12, Exh. 15 at 284:4-12 ("Q: What you had in mind when you conceived of the '606 ideas was a kiosk-type situation, right? A: Mostly that was, yes. Q: And that's a situation where I come up to, for example, a kiosk in an airport and I can use a browser, for example, to access my private data. And I want to make sure that data does not remain for the next guy, is that

Two features distinguish the accused products from the invention claimed in the '606 patent: (a) unlike the claimed invention, the accused products do not delete "temporarily stored" information each time upon logout and (b) unlike in the claimed invention, the accused products installed on a smart phone do not comprise an "untrusted" client site.

The initial shortcoming is fundamentally a matter of claim construction. The court construed the term "temporary storage" to mean "storage location for data that is deleted each time upon logout."[26] Good has alleged that the accused products place three types of workspace data in temporary storage on a smart phone: (1) Personal Information Management data, (2) Microsoft SharePoint data and (3) AppConnect data.[27] Both parties' experts agree that none of these three functionalities put data in any storage location that is deleted each time a user executes a logout command.[28]

Where the parties fundamentally disagree is on what else might constitute a "logout." Good contends that logout also includes server-initiated unenrollment of a device from the system.[29] Good leans heavily on language in the patent that the server can send an "end session

---

right? A: That was the main impetus behind this, yes."); Docket No. 218-14, Exh. 30 (applicant describing "claimed embodiments" as "enabl[ing] a traveling user to log on from any client site that includes a workspace data manager configured to perform these steps."); Docket No. 219-12, Exh. 16 at 32-33 (Good's technical expert stating that "[t]he '606 patent describes a method of accessing personal information on a public kiosk by automatically deleting the personal information after the user has finished using it."); Docket No. 219-12, Exh. 17 at 36 (Good's proposed construction for "untrusted client site" was "a computer expected to be shared by users who are not authorized to access data from the remote site."); Docket No. 219-12, Exh. 18 at 11 (Good arguing "the claimed client is 'untrusted' because it is expected to be shared by other users, hence the automatic deletion mechanism to avoid the possibility that 'unprivileged' users sharing the same computer may be exposed to another user's data."); Docket No. 219-8 at ¶¶ 3-6.

[26] *See* Docket No. 135.

[27] Docket Nos. 255-7, 255-8, Exh. 2 at Sec. IX.O.

[28] *See* Docket No. 219-8 at ¶¶ 10-12; Docket No. 219-14, Exh. 28 at 271:11-272:3, 273:23-276:6; Docket No. 219-9, Exh. 3 at 17-18; Docket No. 219-7 at ¶ 8.

[29] *See* Docket No. 255-4 at 15-16. *See also* Docket No. 218-5, Exh. 20 at 2:40-42 (de-instantiator initiated "upon logout"), 11:11-15 (de-instantiator initiated after "receiving an 'end session' or 'unborrow me' request"); Docket No. 254-12, Exh. 10 at 213-15; Docket No. 255-19, Exh. 11 at 327:10-335:15.

request."[30] But this language says nothing that equates this type of request with logout. In fact, other language in the patent plainly associates log out—the function in dispute—with a user-based identification and password rather than any server-based process.[31] In addition, Good's construction would render the term "temporary" superfluous. Under Good's construction, deletion upon logout would include the one-time deletion of information that has been on the mobile device the entire time that the application has been on the device.[32] The whole point of deletion each time upon logout in the invention is to delete less than that.[33]

As to whether a smart phone secured by the accused products is an "untrusted client," again, the issue is fundamentally one of claim construction. The court previously construed the claimed invention's untrusted client site as a "computer accessible to unprivileged users, no matter the format of a workspace data manager or the presence of a network firewall."[34] The parties do not dispute that a smart phone qualifies as a computer under this construction. The dispute is

---

[30] Docket No. 254-12, Exh. 10 at ¶¶ 673-74.

[31] *See* Docket No. 103 at 7; Docket Nos. 218-5, 218-6, Exh. 7 at 6:34-55 (describing part of embodiment as providing user identification and authentication information to the global server, later followed by a logout); 8:52-61 (describing security module within embodiment as including "routines for obtaining user identification and authentication using such techniques as obtaining login and password information . . . The security module 725 performs identification and authentication techniques to confirm authorization by the user to access the workspace data 135 stored on the global server."); 9:32-10:39 (both Outlook and Lotus Notes embodiments described as requiring a user to enter a login and password, followed later with a logout); 10:50-54 (describing FIG. 8 as requiring login and password information from the user, "[i]f global server fails to identify or authenticate the user, then the method 800 ends."); Docket No. 219-8 at ¶ 8.

[32] *See* Docket Nos. 218-5, 218-6, Exh. 7 at 11:11-16 ("Upon receiving an 'end session' or 'unborrow me' request, the de-instantiator initiates the general synchronization module . . . the de-instantiator in step 860 deletes the workspace data on the client and deletes all records of the matter."); 11:8-10 ("Until an 'end session' request is received, the method 800 returns to step 830 to enable continued data review and manipulation."); 9:32-10:39 (describing deletion of data at the end of a user session using the Outlook and Lotus Organizer embodiments).

[33] Good's alternate theory that the temporary storage limitation is met by MobileIron's multi-user iOS feature is similarly deficient. As MobileIron points out, Good offers no proof from its expert or anyone else of any testing of the feature to assess whether it meets the temporary storage limitation. *See* Docket No. 219-9, Exh. 3 at 18. The Federal Circuit has long held that an expert's conclusory opinions, without any further support, are insufficient to avoid summary judgment. *See, e.g., Amstar Corp. v. Envirotech Corp.*, 823 F.2d 1538, 1545 (Fed. Cir. 1987).

[34] *See* Docket No. 135.

whether Good is correct that this construction of "untrusted client" includes within its scope any smart phone that is capable of being lost or stolen at any time, or in the possession of a former employee.[35] The major problem for Good is that the specification specifically distinguishes "work clients" and "home clients" from "remote clients" that Good agrees are the "untrusted clients."[36] Good's construction would obliterate this distinction, because work clients and home clients also can be lost or stolen.

Second, no reasonable jury could find that claims 1, 10 and 21 of the '606 patent are supported by sufficient written description. "The purpose of the Written Description requirement is to ensure that the scope of right to exclude, as set forth in the claims, does not overreach the scope of the inventor's construction to the field of art as described in the patient specification."[37] "[T]he hallmark of written description is disclosure."[38] "[T]he test for sufficiency is whether the disclosure of the application relied upon reasonably conveys to those skilled in the art that the inventor had possession of the claimed subject matter as of the filing date," and the "specification itself" must demonstrate such possession.[39] "Assessing 'possession as shown in the disclosure' requires an 'objective inquiry into the four corners of the specification.'"[40] "Compliance with the written description requirement is a question of fact.[41]

While the original claims of the '606 patent required only "an untrusted client site," during reexamination the inventors added language to require "a smart phone, defining an untrusted client site."[42] But nowhere in the specification does the term "smart phone" appear—a classic marker of

[35] Docket No. 255-4 at 20:9-18.

[36] Docket Nos. 218-5, 218-6, Ex. 7, FIG. 1, at 110, 115, 120; FIG. 4; 4:6-37, 5:59-6:21.

[37] *Atl. Research Marketing Sys. v. Troy*, 659 F.3d 1345, 1354 (Fed. Cir. 2011).

[38] *Ariad Pharm., Inc. v. Eli Lilly & Co.*, 598 F.3d 1336, 1351 (Fed. Cir. 2010).

[39] *Id.* at 1351-52.

[40] *Novozymes A/S v. DuPont Nutrition Biosciences APS*, 723 F.3d 1336, 1344 (Fed. Cir. 2013) (citations omitted).

[41] *Id.* at 1351.

[42] Docket Nos. 218-5, 218-6, Exh. 7 at 1:28-29, 1:58-59, 2:46-47.

a written description problem. Good concedes this point, but counters that the specification nevertheless "describes the hallmarks of a smart phone."[43] But even if the specification need not use the exact words of the claimed invention, it "must do more than merely disclose that which would render the claimed invention obvious."[44] The "hallmarks" Good points to are nothing more than the generic requirements of any computer allowing remote access. Nor is there any merit to Good's reliance on certain incorporated reference patents. "To incorporate material by reference, the host document must identify with particularity what specific material it incorporates and clearly indicate where that material is found in the various documents."[45] Even if the '606 patent identified with particularity the material Good relies on—which it does not—the incorporated patents make no distinction between trusted and untrusted sites; the sites are always trusted.[46] Coupled with the inventor's own testimony that a smart phone is trusted,[47] no reasonable jury could deny that, by clear and convincing evidence, claims 1, 10 and 21 of the '606 patent are invalid for lack of sufficient description.[48]

---

[43] *See* Docket No. 255-4 at 32; Docket Nos. 218-5, 218-6, Exh. 7 at 1:45-48 (the '606 patent describes that "[d]ata accessibility and consistency are significant concerns" for a "roaming user, i.e., a user who travels to a remote location [and] needs to review or manipulate data such as an e-mail"); *id.* at 5:59-6:5, 7:37-42 (to accommodate the "roaming users" the '606 patent teaches an "untrusted client"—referred to as a "remote client" in the specification—that includes "a processor 405," "input device 415," "output device 420," "data storage 425," "internal storage 430 such as RAM," a "communications interface," "an operating system 440" and a "PIM 170" which can be used for reading, replying to, forwarding and writing new emails.); *id.* at 3:11-14, 12:23 (the '606 patent further reaches "access and synchronization of data across . . . network firewalls" and that the connections for such access and synchronization can be "wireless.").

[44] *ICU Med., Inc. v. Alaris Med. Sys., Inc.*, 558 F.3d 1368, 1377 (Fed. Cir. 2009).

[45] *Xenon Environmental, Inc. v. U.S. Fitter Corp.*, 506 F.3d 1370, 1378 (Fed. Cir. 2007).

[46] *See generally* Docket Nos. 218-10, 218-11, 218-12, Exhs. 22-24.

[47] *See* Docket No. 219-11, Exh. 12 at 89:18-90:1; *Voice Tech. Grp., Inc. v. VMC Sys., Inc.*, 164 F.3d 605, 615 (Fed. Cir. 1999) ("An inventor is a competent witness to explain the invention and what was intended to be conveyed in the specification and covered by the claims. The testimony of the inventor may also provide background information, including explanation of the problems that existed at the time the invention was made and the inventor's solution to these problems.").

[48] The court does not reach invalidity of claims 1 and 21 of the '606 patent based on lack of written description of "at the remote site."

Third, Good has not produced evidence that even hints that MobileIron willfully infringed, rendering summary judgment appropriate. To establish willfulness, "a patentee must show by clear and convincing evidence that (1) the infringer acted despite an objectively high likelihood that its actions constituted infringement of a valid patent," and (2) the objectively-defined risk "was either known or so obvious that it should have been known to the accused infringer."[49] The objective prong "should always be decided as a matter of law by the judge"[50] and as a "predicate to the jury's consideration of the subjective prong."[51] A finding of willfulness must be made in light of the totality of the circumstances.[52] "Should the court determine that the infringer's reliance on a defense was not objectively reckless, it cannot send the question of willfulness to the jury."[53]

With respect to pre-suit willfulness, Good cannot show that MobileIron had pre-suit knowledge of Good's patents. The best Good can point to is some internal MobileIron emails that discuss suits Good had filed against other defendants, evidence that MobileIron performed competitive analysis on Good as early as 2008 and evidence that MobileIron sent a representative to a Good event under a false name.[54] But at most, this suggests that MobileIron could have known about Good's patents, not that MobileIron actually knew.[55] In any event, showing

---

[49] *In re Seagate Tech., LLC*, 497 F.3d 1360, 1371 (Fed. Cir. 2007) (en banc).

[50] *Bard Peripheral Vascular, Inc. v. W.L. Gore & Assocs.*, 682 F.3d 1003, 1008 (Fed. Cir. 2012).

[51] *Powell v. Home Depot U.S.A., Inc.*, 663 F.3d 1221, 1236 (Fed. Cir. 2011) (citing *In re Seagate Tech., LLC*, 497 F.3d at 1371).

[52] *Knorr-Bremse Systeme Fuer Nutzfahrzeuge GmbH v. Dana Corp.*, 383 F.3d 1337, 1342-43 (Fed. Cir. 2004) (en banc).

[53] *Powell*, 663 F.3d at 1236 (citing *In re Seagate Tech., LLC*, 497 F.3d at 1371).

[54] *See* Docket Nos. 255-30, 255-31, 255-32, 255-33, Exhs. 25-28. Good also points to MobileIron interrogatory responses regarding its first knowledge of the patents-in-suit.

[55] This is fundamentally different from what happened in *i4i Ltd. Partnership v. Microsoft Corp.*, 598 F.3d 831 (Fed. Cir. 2010). There, the Federal Circuit found sufficient evidence of willfulness based on, among other things, evidence the accused infringer saw materials citing the asserting patent: "In this case, i4i presented sufficient evidence at trial to prove each prong of the Seagate standard for willfulness. The jury heard that Microsoft employees attended demonstrations of i4i's software, which practiced the '449 patent. Further, the jury learned that Microsoft employees received i4i's sales kit, which identified i4i's software as 'patented' technology and cited the '449 patent. The jury then saw a series of emails between Microsoft employees discussing a marketing email sent by i4i. One of those emails explained that the 'heart' of i4i's software was patented,

knowledge of the patents themselves does not nudge Good over the edge to being able to show willfulness.[56] Good has not shown any indication that, pre-suit, MobileIron knew or should have known that its products infringed Good's patents.

As to post-filing willfulness, Good has again failed to meet its burden. Good did not seek a preliminary injunction, and a "patentee who does not attempt to stop an accused infringer's activities in this manner should not be allowed to accrue enhanced damages based solely on the infringer's post-filing conduct."[57] Even if "*Seagate* did not establish a categorical rule,"[58] upon learning of its potential infringement, MobileIron sought advice of counsel letters to determine whether there was merit to the allegations of infringement.[59] While the parties disagree about whether the opinion letters sufficiently addressed the accused products or whether they were accurate, "[t]hose cases where willful infringement is found despite the reference of an opinion of counsel was either ignored or found to be incompetent."[60] No such facts are evidenced here. Coupled with the fact that Good promises to show recklessness at trial, yet fails to do so now, these circumstances compel this court to grant summary judgment of willful infringement as to both pre-suit and post-filing conduct.

---

again citing the '449 patent. Based on this circumstantial evidence, the jury could have reasonably inferred that Microsoft knew about the '449 patent."

[56] *See Aircraft Tech. Publishers v. Avantext, Inc.*, Case No. 07-cv-04154, 2009 WL 4348334, at *3 n.3 (N.D. Cal. Nov. 19, 2009); *Norian Corp. v. Stryker Corp.*, 363 F.3d 1321, 1332 (Fed. Cir. 2004) ("Willful infringement is not established by the simple fact of infringement, even though Stryker stipulated that it had knowledge of the Norian patents.").

[57] *In re Seagate Tech., LLC*, 497 F.3d at 1374.

[58] *Krippelz v. Ford Motor Co.*, 675 F. Supp. 2d 881, 897 (N.D. Ill. 2009); s*ee also ACCO Brands, Inc. v. PC Guardian Anti-Theft Prods., Inc.*, 592 F. Supp. 2d 1208, 1227 (N.D. Cal. 2008); *accord Monolithic Power Sys., Inc. v. Silergy Corp.*, Case No. 14-cv-01745, 2015 WL 3799533, at *2-3 (N.D. Cal. June 18, 2015).

[59] *See* Docket Nos. 218-14, 219-16, 219-17, 219-18, 219-19, 219-20, 219-21, 219-22, 219-23, 219-24, 219-25, 219-26, 219-27, 219-28, 219-29, 219-30, 219-31, 219-32, 219-33, 219-34, 219-35, 219-36, 219-37, 219-38, 219-39, 219-40, 219-41, 219-42, 219-43, 219-44, 219-45, 219-46, Exhs. 35-40.

[60] *Read v. Portec*, 970 F.3d 818, 828-29 (Fed. Cir. 1992).

Fourth, Good has not presented any evidence to substantiate its claims of indirect infringement. To prove induced infringement, "the patentee must show that the accused inducer took an affirmative act to encourage infringement with the knowledge that the induced acts constitute patent infringement."[61] The same standard applies to contributory infringement.[62] As discussed above, Good has failed to present evidence that MobileIron had knowledge of the patents pre-suit or that MobileIron's various defenses are anything other than reasonable.

Good disputes MobileIron's contention that contributory infringement requires a showing of specific intent to infringe, positing instead that contributory infringement may be inferred from knowledge of the patents and the lack of substantial non-infringing uses.[63] But Good also fails to show that MobileIron's products have no substantial non-infringing uses. Rather, Good seeks to shift the burden to MobileIron to show that there are substantial non-infringing uses. And MobileIron—while arguing that Good is improperly shifting the burden—answers the call by pointing to turning a device over to a new user, rather than exclusively based on wiping a device in response to the device being compromised, as required by the '606 and '219 patents.[64] With regard to the '322 patent, Apps@Work and App Catalog can distribute applications as well as distribute updates.[65] No reasonable jury could find that these uses are "unusual, far-fetched, illusory,

---

[61] *Microsoft Corp. v. DataTern, Inc.*, 755 F.3d 899, 904 (Fed. Cir. 2014) (citing *Global-Tech Appliances, Inc. v. SEBA S.A.*, 131 S. Ct. 2060, 2068 (2011)); *XimpleWare, Inc. v. Versata Software, Inc.*, Case No. 13-cv-05161, 2014 WL 6687219, at *7 (N.D. Cal. Nov. 25, 2014) (the "intent necessary to induce infringement requires more than just intent to cause the acts that produce direct infringement."). *See also Commil USA, LLC v. Cisco Sys., Inc.*, Case No. 13-00896 (U.S. May 26, 2015) (holding that "liability for induced infringement can only attach if the defendant knew of the patent and knew as well that the induced acts constitute patent infringement").

[62] *See Global-Tech Appliances, Inc.*, 131 S. Ct. at 2067.

[63] *See Ricoh Co., Ltd. v. Quanta Computer Inc.*, 550 F.3d 1325, 1338 (Fed. Cir. 2008) ("The purpose of the 'substantial noninfringing use' exception of § 271(c) is to allow determination of instances where the intent to infringe may be presumed based on the distribution of a product that has an unlawful use . . . Unlike contributory infringement, induced infringement liability under § 271(b) requires proof that 'the inducer [has] an affirmative intent to cause direct infringement.'").

[64] Docket No. 267-2, Exh. 43 at 625-27.

[65] Docket No. 267-2, Exh. 41 at ¶¶ 278, 290.

impractical, occasional, aberrant, or experimental."[66] That these uses may otherwise infringe is no matter; unlike with damages, the standard for avoiding indirect infringement is merely substantial non-infringing uses, not non-infringing alternatives altogether. The best Good and its expert can do is to offer the conclusory statement that "MobileIron would know [its products] had no non-infringing uses."[67] An expert's conclusory statements, however, are not enough to create a genuine dispute, especially when the expert acknowledges various non-infringing uses.[68] On this record, no reasonable jury could return a finding of indirect infringement.

Fifth, there is a genuine issue whether MobileIron infringes the '386 patent. The issue centers on whether MobileIron's accused products meet the requirement that they include a "rules engine being triggered to gather [] information repeatedly on the basis of a monitoring time interval."[69] Notably, the parties did not present this claim term for construction earlier. But where, as here, the parties dispute not merely the meaning of words themselves, but the scope that should be encompassed by those words, the court is not free to punt the issue.[70]

The issue is more specifically whether a triggering event can be considered a monitoring time interval. MobileIron and its expert Earl Sacerdoti urge that one of ordinary skill in the art, reading the claim limitation in the context of the specification, would understand that the repeated gathering of information take place at a specific time interval.[71] Sacerdoti further explains that this is distinct from event-based monitoring, whereby monitoring is based on an event that occurs at irregular, unpredictable times.[72] Not surprisingly, MobileIron's products do not gather information at any regular or predictable time.

---

[66] *Vita-Mix Corp. v. Basic Holding, Inc.*, 581 F.3d 1317, 1327 (Fed. Cir. 2009).

[67] Docket No. 219-9, Exh. 3 at ¶ 310.

[68] *See id.* at Exh. A at 20-21, Exh. C at 9-10.

[69] *See* Docket No. 218-3, Exh. 1 at 7:31-33.

[70] *See 02 Micro Intern. Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1360-63 (Fed. Cir. 2008).

[71] *See* Docket No. 219-6 at ¶¶ 13-22.

[72] *See id.*

The problem for MobileIron and Sacerdoti is that the specification is explicit that the time interval may include such irregular and unpredictable events as start-up and installation of components.[73] No set frequency based on seconds, minutes or hours is required; so long as the information is gathered repeatedly, the invention is completed.[74] In fact, a specific embodiment includes both event-based and time-based monitoring intervals:

> In one embodiment, such a periodic monitoring session may occur at various time intervals including, upon start-up of the wireless device, once a day, once a week, and upon installation of any components or applications on the wireless device.[75]

By urging a construction that would exclude a disclosed embodiment, MobileIron would improperly limit the claim.[76]

MobileIron does not seriously dispute that the specification teaches that a periodic monitoring session, or time interval, may be defined without a set frequency as noted above. Instead, MobileIron argues that the inventors' teaching is "confusing" or at odds with the plain and ordinary meaning of the disputed language. But there is nothing confusing here at all; the ordinarily skilled artisan is on full notice that while a set frequency may define the period of monitoring, it could just as well be defined by events such as start-up or the installation of components or applications.[77]

---

[73] *See* Docket No. 255-5, Exh. 1 at 15:2-18:25.

[74] *See id.* at 16:25-17:2.

[75] *See* Docket No. 218-3, Exh. 1 at 6:6-10.

[76] *See Broadcom Corp. v. Emulex Corp.*, 732 F.3d 1325, 1333 (Fed. Cir. 2013) (rejecting non-infringement argument because the suggested restriction "would improperly exclude a disclosed embodiment" and "the specification shows that the [disputed] claim term does not limit the invention" as suggested).

[77] *Cf. Elekta Instruments S.A. v. O.U.R. Scientific Int'l*, 214 F.3d 1302, 1307 (Fed. Cir. 2000). With respect to Claim 8, a genuine issue remains whether the accused products' "device inactivity timer" is checked each time the device is started up. *See* Docket No. 255-10, Exh. 3 at 6. With respect to Claim 9, a genuine issue remains whether the "set of rules" transmitted from the server to the wireless device and the installation of "components" on the wireless device on which the monitoring time interval depends are the "profiles" or "policies" required. *See id.* at 12-13; Docket No. 255-5, Exh. 1 at 234:1-235:3. Claim 9 remains narrower than Claim 1, upon which it depends, because in light of the specific claim type of "monitoring claim interval" required by Claim 9 the claims have at least one different claim limitation. *See Kraft Foods, Inc. v. Int'l Trading Co.*, 203 F.3d 1362, 1368 (Fed. Cir. 2000) ("That the claims are presumed to differ in scope does not mean

Sixth, there is a disputed question of fact as to whether MobileIron infringes the '322 patent. The issue here is about whether any of the accused products send a message that indicates "one or more files within the updates to download." MobileIron argues that its products send updates themselves or links to updates themselves rather than any files within the updates and that Good disclaimed such functionality during prosecution to avoid a prior art rejection.[78] But Good's claims never specified messages indicating updates prior to amendment, and so they could not have been disclaimed.[79] Rather, before their amendment the claims specified "receiving a Universal Resource Locator [] from a web-based software server indicating a location of the updates,"[80] which is distinct from indicating the updates themselves.

MobileIron's argument is a version of the same argument it made at claim construction, when MobileIron argued that the disputed language be construed as "message identifying specific file[s] within an update package that are appropriate for the particular device to [download/upload]."[81] The court instead adopted a construction of "message indicating at least one file within the updates to [download/upload]."[82] The parties agree that MobileIron's accused products send messages that identify the .apk or .ipa files.[83] A reasonable jury could find that this is sufficient.

---

that every limitation must be distinguished from its counterpart in another claim, but only that at least one limitation must differ.").

[78] Docket No. 218-4, Exh. 6 at 2.

[79] *See id.*

[80] *Id.*

[81] Docket No. 107 at 22.

[82] *See* Docket No. 135.

[83] *See* Docket No. 219-7 at ¶¶ 14-15. For example, Hugh Smith's expert report identifies source code evidence, documents and deposition testimony that the accused products create install application commands that are downloaded by MobileIron managed wireless devices that identify the .ipa and .apk files. Docket No. 255-15, Exh. 6 at 59:9-11, 62:9-11, Docket No. 255-16, Exh. 7 at 34:15-35:3; Docket No. 255-17, Exh. 8, Docket No. 255-18, Exh. 9 ("During check-in, we would send a managed app install command down to the iOS device, and that would kick off the update process") (describing MobileIron protocol for application installs).

Seventh, there is a disputed question of fact as to whether MobileIron infringes the '219 patent. Two claimed features are at issue: the distinction between synchronized and non-synchronized information and whether MobileIron's software includes a list as the '219 patent requires. Once again, further claim construction is required.

As to synchronization, the preamble to claim 1 of the '219 patent teaches:

> A method of controlling access to data including a plurality of sets of data, the plurality of sets of data comprising a first set of data items to be synchronized between a server system and a remote device, the remote device being remote from the server system, and a second, different, set of data items held on the remote device, the first set of data items including data items whose values are updated at the server system in response to changes thereto on the remote device, the second set of data items including data items whose values are not updated at the server system in response to changes thereto on the remote device, the remote device providing access to at least some of the data held thereon.[84]

MobileIron argues that the plain language of this text requires two separate sets of information: a first set that is synchronized to the server and a second set that resides on the remote device and is not synchronized to the server.[85] As MobileIron sees it, the first set cannot include any non-synchronized data and the second set can include no synchronized data. If this construction were to carry the day, MobileIron's products would not infringe the '219 patent because MobileIron's products are not so configured.[86]

Unfortunately for MobileIron, this construction ignores the language of the claim that specifies that the first set "includ[es]" synchronized data. In both ordinary usage and the particular vernacular of the patent world, the word "includes" is open-ended and permits more than that which follows.[87] The specification further makes clear that data in the first set that are only

---

[84] Docket No. 218-13, Exh. 25 at 22:35-47.

[85] *See* Docket No. 219-5 at 37-38.

[86] *See* Docket No. 219-14, Exh. 28 at 361:3-12.

[87] *See Hewlett-Packard Co. v. Repeat-O-Type Stencil Mfg. Corp.*, 123 F.3d 1445, 1451 (Fed. Cir. 1997) ("The claim term 'including' is synonymous with 'comprising,' thereby permitting the inclusion of unnamed components.").

updated on the remote device in response to changes on the server are non-synchronized.[88] At the end of the day, Good offers the better construction: that the first and second sets of data are distinct based on personal versus non-personal information, and non-personal data can include non-synchronized data in addition to non-personal, synchronized data.[89]

As to the issue of whether MobileIron's product includes lists as contemplated by the '219 patent, once again the court is effectively asked to adopt a claim construction it previously rejected. At claim construction, MobileIron urged a construction of "list" as "enumeration of the data items with an indication for each data item whether it belongs to the first set [and/or] the second set."[90] The court declined, choosing instead to construe the term as having its plain and ordinary meaning.[91] Good offers competent evidence that it can prove that MobileIron's products satisfy this meaning because they "contain[] a pointer to the list of apps and so [] contain[] the list of apps. A list of a list is a list."[92] This is a classic dispute that requires a jury to resolve.

The parties also genuinely disagree about how many lists MobileIron's products have. MobileIron contends that it only has one list. But Good offers substantial evidence that MobileIron's software includes a list that identifies all managed applications installed on the device.[93] This software is used to retire a device and thus identifies all applications and their associated content that need to be deleted.[94] According to Good's expert, all information excluded

---

[88] *See* Docket No. 218-13, Exh. 19 at 11:20-24 ("[I]n an alternative embodiment, the non-synchronized data type 510 can actually be one-way synchronized. That is, changes in server data 115 will change the remote device data 121, but not vice versa.").

[89] *See id.* at 1:11-13 ("The remote device data 121 include non-synchronized remote device data 510, synchronized remote device data 520, and personally owned remote device data 530."). Nor does anything in the prosecution history clearly and unmistakably disclaim the full scope of this claimed first set of data. *See SanDisk Corp. v. Memorex Prods., Inc.*, 415 F.3d 1278, 1286-87 (Fed. Cir. 2005).

[90] Docket No. 107 at 13.

[91] *See* Docket No. 135.

[92] Docket No. 255-19, Exh. 11 at 377:16-19.

[93] Docket No. 255-25, Exh. 16 at 7-11.

[94] *Id.* at 8-9.

from that first list is necessarily included in the second set of information, conforming to the requirements of the '219 patent. While MobileIron disputes that an inferred list can be a list at all, especially since the patent contemplates a plurality of data sets,[95] a reasonable jury could conclude that Good's expert has the better of the argument.

Eighth, Good is entitled to present its doctrine of equivalents case at trial. In *Festo Corp. v. Shoketsu Kinzoku Kogyo Kabushiki Co., Ltd.*, the Supreme Court held that in order to pursue a DOE theory as to claims that were amended during prosecution, the patentee must either (1) prove that alleged equivalents were unforeseeable at the time of amendment, (2) prove that the amendments are only tangentially related to the equivalent in question or (3) offer some other compelling reason as to why the equivalent could not have been expressly claimed.[96] MobileIron argues that all six of Good's DOE allegations should be precluded because Smith concluded—without basis—that "nothing within the [patents] or the File Histor[y] precludes such a finding of equivalents under the Doctrine of Equivalents,"[97] which cannot satisfy the heavy burden under *Festo*. But upon careful consideration, each equivalent at issue passes muster.

As to the '606 patent, Smith alleges that the literal scope of the "request to access data temporarily from a remote site" limitation is equivalent to "requesting data from a remote site that may encompass one or more physical locations."[98] The DOE reference here only pertains to the term "remote site," which was not added during prosecution.[99] As such, *Festo* does not apply. Similarly, Smith's other DOE allegation as to the '606 patent—which alleges that the literal scope of the "temporary storage" limitation, that requires deleting the data from the storage location upon each logout, is equivalent to encrypting the data upon a user exiting the interface—is only

---

[95] Docket No. 219-5 at 40-41.

[96] *Integrated Tech. Corp. v. Rudolph Techs., Inc.*, 734 F.3d 1352, 1356 (Fed. Cir. 2013) (citing *Festo Corp.*, 535 U.S. 722, 740-41 (2002)).

[97] *See, e.g.*, Docket No. 219-9, Exh. 3, Exh. A at 11, 18.

[98] *See* Docket No. 255-21, Exh. 12 at 11.

[99] *See* Docket No. 254-17, Exh. 15.

tangentially relevant because whether the information is deleted or encrypted, the end result is that the user no longer has access to the information.[100] Again, this reasoning comports with *Festo*.

With regard to the '219 patent, Smith alleges that the literal scope of the "list identifying each data item as belonging to the first set or the second set" limitation is equivalent to a list in which a data item is identified "by way of associated application" or is equivalent to a list where "only one set is specified and the other is specified by implication."[101] Because the amendment was made to overcome a written description rejection rather than to overcome prior art,[102] *Festo* does not apply.

As to the '386 patent, Smith alleges that the literal scope of the "maintaining particular settings associated with the service" limitation is equivalent to creating, modifying or deleting settings or is equivalent to managing other settings at the same time as those associated with the service.[103] Because the relevant amendments—whether the deletion of settings is equivalent to maintaining settings and whether other settings can be managed at the same time as those associated with the service—are unrelated to the arguments put forth to overcome the prior art,[104] *Festo* is again inapplicable.

As to the '322 patent, Smith alleges that the literal scope of the "searching a compatibility matrix for rules associated with each update" limitation is equivalent to searching a compatibility matrix that is external to the update.[105] Because there was no compatibility matrix at issue in any of the asserted prior art, the arguments asserted to overcome that prior art are unrelated to the theories set forth here.[106] Again, *Festo* does not apply.

---

[100] *See* Docket No. 255-21, Exh. 12 at 18-19.

[101] *See* Docket No. 255-25, Exh. 16 at 10-11.

[102] *See* Docket No. 254-17, Exh. 15.

[103] *See* Docket No. 255-23, Exh. 14 at ¶ 21.

[104] *See* Docket No. 254-17, Exh. 15.

[105] *See* Docket No. 255-14, Exh. 5 at 12.

[106] *See* Docket No. 254-17, Exh. 15.

IV.

The motion is GRANTED-IN-PART.

SO ORDERED.

Dated: June 30, 2015

PAUL S. GREWAL
United States Magistrate Judge